2

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-023154
(43)Date of publication of application : 22.01.2004

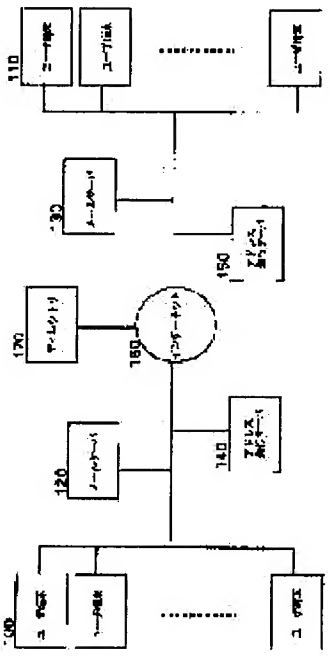
(51)Int.Cl. H04L 12/58
G06F 13/00
G09C 1/00

(21)Application number : 2002-171571
(22)Date of filing : 12.06.2002

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : TSURUOKA YUKIO
ONO SATOSHI
HISADA YUSUKE

(54) ELECTRONIC MAIL SYSTEM AND METHOD FOR PROCESSING ELECTRONIC MAIL

(57)Abstract:



PROBLEM TO BE SOLVED: To provide an electronic mail system and a method for processing an electronic mail wherein address issue servers for issuing electronic mail addresses and mail servers for delivering mails are provided and a plurality of the servers distributingly and efficiently perform error processing such as processing to be applied to the mail whose destination is not clear and the mail whose reception is rejected by a recipient.
SOLUTION: Each of the address issue servers includes: a means for entering control information; a key storage means; a means for calculating inspection information to inspect the propriety of an address on the basis of the control information and a key; and a means that generates an address to which the control information and the inspection information are embedded and transmits the resulting address to a user's terminal.
Each of the mail servers includes: a means that extracts the control information and the inspection information on the basis of a sender address and a recipient address of mail; a key storage means; a means that discriminates the propriety of the mail delivery on the basis of the extracted control information and inspection information and the key; and a means for performing the mail delivery processing or the error processing on the basis of the propriety discrimination result.

15 pgs

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-23154
(P2004-23154A)
(43)公開日　平成16年1月22日(2004.1.22)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	12/58	H04L	12/58	100F	5J104
G06F	13/00	G06F	13/00	630A	5K030
G09C	1/00	G09C	1/00	640D	

審査請求 未請求　請求項の数 4　OL　（全 14 頁）

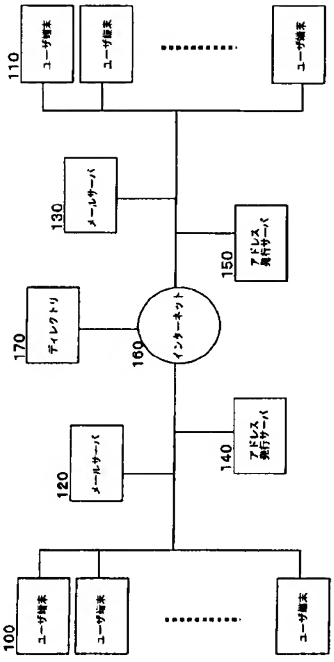
(21)出願番号　特願2002-171571(P2002-171571)
(22)出願日　平成14年6月12日(2002.6.12)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100074930
弁理士　山本　恵一
(72)発明者　鶴岡　行雄
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　小野　諭
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　久田　裕介
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Fターム(参考)　5J104 PA08
5K030 GA15 HA06 HB08 LC15 LD13

(54)【発明の名称】電子メールシステム及び電子メール処理方法

(57)【要約】
【課題】電子メールアドレスを発行するアドレス発行サーバと、メールを配送するメールサーバとを有する電子メールシステム及び処理方法であって、宛先不明又は受信者により受信を拒否されるメール等のエラー処理を、複数のサーバで分散して効率的に行うものを提供する。
【解決手段】アドレス発行サーバは、制御情報を入力する手段と、鍵記憶手段と、制御情報及び鍵からアドレスの正当性を検査するための検査情報を計算する手段と、制御情報及び検査情報を埋め込んだアドレスを生成し、ユーザの端末へ送信する手段とを有し、メールサーバは、メールの送信者アドレス及び受信者アドレスから制御情報及び検査情報を抽出する手段と、鍵記憶手段と、抽出された該制御情報及び該検査情報と該鍵とからメール配送の可否判断を行う手段と、可否判断に基づいてメール配送処理又はエラー処理を行う手段とを有する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
送信ユーザから受信ユーザへメッセージを配送するために、ユーザに電子メールアドレスを発行するアドレス発行サーバと、メールを配送するメールサーバとを有する電子メールシステムであって、
前記アドレス発行サーバは、制御情報（ｅ１，ｅ２，ｅ３，ｅ４，ｅ５）を入力する手段と、鍵を記憶する手段と、該制御情報と該鍵とからアドレスの正当性を検査するための検査情報（ｅ６）を計算する手段と、前記制御情報及び前記検査情報を埋め込んだアドレスを生成する手段と、生成した該アドレスをユーザに通知する手段とを有し、
前記メールサーバは、処理するメールの送信者アドレス及び受信者アドレスから前記制御情報及び前記検査情報を抽出する手段と、鍵を記憶する手段と、抽出された該制御情報及び該検査情報と該鍵とからメール配送の可否判断を行う手段と、該可否判断に基づいてメール配送処理又はエラー処理を行う手段とを有することを特徴とする電子メールシステム。
【請求項２】
前記制御情報は、発行するアドレスに下記の情報（ｅ２，ｅ３，ｅ４，ｅ５）及び前記検査情報（ｅ６）を埋め込む形式及びそれらの情報の利用方法を表すフォーマット情報（ｅ１）と、発行するアドレスが有効となる条件を表す有効条件（ｅ２）と、発行するアドレスへメールを送ることができるユーザを表す送信者識別子（ｅ３）と、発行するアドレスへ送られたメールを受け取るユーザを表す受信者識別子（ｅ４）と、その他の目的に用いる付加情報（ｅ５）とを、それぞれ必要に応じて有することを特徴とする請求項１に記載の電子メールシステム。
【請求項３】
送信ユーザから受信ユーザへメッセージを配送するために、ユーザに電子メールアドレスを発行するアドレス発行処理ステップと、メールを配送するメール配送処理ステップとを有する電子メール処理方法であって、
前記アドレス発行処理ステップは、鍵を記憶しており、制御情報（ｅ１，ｅ２，ｅ３，ｅ４，ｅ５）を入力し、該制御情報と該鍵とからアドレスの正当性を検査するための検査情報（ｅ６）を計算し、前記制御情報及び前記検査情報を埋め込んだアドレスを生成し、生成した該アドレスをユーザに通知し、
前記メール配信処理ステップは、鍵を記憶しており、処理するメールの送信者アドレス及び受信者アドレスから前記制御情報及び前記検査情報を抽出し、抽出された該制御情報及び該検査情報と該鍵とからメール配送の可否判断を行い、該可否判断に基づいてメール配送処理又はエラー処理を行う
ことを特徴とする電子メール処理方法。
【請求項４】
前記制御情報は、発行するアドレスに下記の情報（ｅ２，ｅ３，ｅ４，ｅ５）及び前記検査情報（ｅ６）を埋め込む形式及びそれらの情報の利用方法を表すフォーマット情報（ｅ１）と、発行するアドレスが有効となる条件を表す有効条件（ｅ２）と、発行するアドレスへメールを送ることができるユーザを表す送信者識別子（ｅ３）と、発行するアドレスへ送られたメールを受け取るユーザを表す受信者識別子（ｅ４）と、その他の目的に用いる付加情報（ｅ５）とを、それぞれ必要に応じて有することを特徴とする請求項３に記載の電子メール処理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、電子メール（以下「メール」という）システムにおいて、宛先不明のメールや受信者が受信を拒否したメール等の無効なメールを効率的に処理するシステム及び方法に関する。特に、電子メールアドレス（以下「アドレス」という）に情報を埋め込み、メール配送時にその埋め込まれた情報を検査することによって、無効なメールを排除する機能

や、メール送受信者に有益な情報を提供する機能を実現する。

【０００２】

【従来の技術】

受信者が望まない送信者からのメールを排除する方法として、従来、アクセス制御リスト等を用いたフィルタが使われている。フィルタとは、処理するメールについて、予め設定した条件に基づき配送処理（正常処理）又はエラー処理を行うものとする。アクセス制御リストには、メールを送ってもよいユーザの集合（ホワイトリスト）を指定する方法や、メールを送って欲しくないユーザの集合（ブラックリスト）を指定する方法がある。そのアクセス制御リストを含むフィルタの構成については、例えば、文献「電子メールプロトコル詳説」（ＩＳＢＮ４－８９４７１－２９０－３）の第７章の図７．１に示されている。その図によれば、フィルタ処理は、受信者側のメールサーバ（図のＭＴＡ及びＭＤＡ）又はユーザ端末（図のＭＵＡ）で行われている。また、電子メールの内容によるフィルタ技術については、特開２０００－３５３１３３号公報「電子メッセージの望ましくない送信または受信を妨害するためのシステムおよび方法」に記載されており、その図２にはフィルタの構成が示されている。その図において、メールは、受信者側のメールサーバ２０８で中継され、同サーバでフィルタ処理され、ユーザに配送される。以上のように、従来の方法によれば、メールのフィルタ処理を、受信者端末又は受信者側のメールサーバで行うものである。

【０００３】

【発明が解決しようとする課題】

しかしながら、上述した従来のシステムでは、次のような問題がある。

【０００４】

第１の問題点は、宛先不明のメールや受信者により受信を拒否されるメールが大量に送信されてきた場合に、受信者側のメールサーバの負荷が高くなるということである。その理由は、受信者側のメールサーバで一元的にフィルタ処理を行うためである。

【０００５】

第２の問題点は、指定した宛先まで配送されないメールのために、無駄なトラフィックが生じるということである。その理由は、メールが宛先に指定した受信者又はその直前に位置する受信者側のメールサーバまで到達しないと、受信の可否判断ができないためである。受信拒否となった場合には、そこまでのトラフィックは無駄になり、更にエラーメールの返送も同様のトラフィックを生じる。

【０００６】

第３の問題点は、アドレスを一時的な目的のために用いた場合、目的が終了しアドレスが無効になったことを送信者に知らせる手段が無いことである。

【０００７】

第４の問題点は、アドレスが漏洩したときに、漏洩元を知る方法が無いことである。

【０００８】

そこで、本発明の目的は、宛先不明のメールや受信者により受信を拒否されるメール等のエラー処理を、複数のサーバで分散して効率的に行うシステムを提供することにある。また、本発明の他の目的は、アドレスに情報を埋め込むことで、上記の第３と第４の問題点を解決するほか、メールの送信者及び受信者へ有益な情報を与えることを可能とするシステムを提供することにある。

【０００９】

【課題を解決するための手段】

本発明によれば、送信ユーザから受信ユーザへメッセージを配送するために、ユーザに電子メールアドレスを発行するアドレス発行サーバと、メールを配送するメールサーバとを有する電子メールシステムであって、

アドレス発行サーバは、制御情報（ｅ１，ｅ２，ｅ３，ｅ４，ｅ５）を入力する手段と、鍵を記憶する手段と、該制御情報と該鍵とからアドレスの正当性を検査するための検査情報（ｅ６）を計算する手段と、制御情報及び検査情報を埋め込んだアドレスを生成する手

段と、生成した該アドレスをユーザに通知する手段とを有し、
メールサーバは、処理するメールの送信者アドレス及び受信者アドレスから制御情報及び検査情報を抽出する手段と、鍵を記憶する手段と、抽出された該制御情報及び該検査情報と該鍵とからメール配送の可否判断を行う手段と、該可否判断に基づいてメール配送処理又はエラー処理を行う手段とを有することを特徴とする。

【００１０】

本発明の電子メールシステムの他の実施形態によれば、
制御情報は、発行するアドレスに下記の情報（ｅ２，ｅ３，ｅ４，ｅ５）及び検査情報（ｅ６）を埋め込む形式及びそれらの情報の利用方法を表すフォーマット情報（ｅ１）と、発行するアドレスが有効となる条件を表す有効条件（ｅ２）と、発行するアドレスへメールを送ることができるユーザを表す送信者識別子（ｅ３）と、発行するアドレスへ送られたメールを受け取るユーザを表す受信者識別子（ｅ４）と、その他の目的に用いる付加情報（ｅ５）とを、それぞれ必要に応じて有することも好ましい。

【００１１】

また、本発明の電子メール処理方法によれば、送信ユーザから受信ユーザへメッセージを配送するために、ユーザに電子メールアドレスを発行するアドレス発行処理ステップと、メールを配送するメール配送処理ステップとを有する電子メール処理方法であって、
アドレス発行処理ステップは、鍵を記憶しており、制御情報（ｅ１，ｅ２，ｅ３，ｅ４，ｅ５）を入力し、該制御情報と該鍵とからアドレスの正当性を検査するための検査情報（ｅ６）を計算し、制御情報及び検査情報を埋め込んだアドレスを生成し、生成した該アドレスをユーザに通知し、
メール配信処理ステップは、鍵を記憶しており、処理するメールの送信者アドレス及び受信者アドレスから制御情報及び検査情報を抽出し、抽出された該制御情報及び該検査情報と該鍵とからメール配送の可否判断を行い、該可否判断に基づいてメール配送処理又はエラー処理を行う
ことを特徴とする。

【００１２】

本発明の電子メール処理方法の他の実施形態によれば、
制御情報は、発行するアドレスに下記の情報（ｅ２，ｅ３，ｅ４，ｅ５）及び検査情報（ｅ６）を埋め込む形式及びそれらの情報の利用方法を表すフォーマット情報（ｅ１）と、発行するアドレスが有効となる条件を表す有効条件（ｅ２）と、発行するアドレスへメールを送ることができるユーザを表す送信者識別子（ｅ３）と、発行するアドレスへ送られたメールを受け取るユーザを表す受信者識別子（ｅ４）と、その他の目的に用いる付加情報（ｅ５）とを、それぞれ必要に応じて有することも好ましい。

【００１３】

前述した本発明により、メール受信者に関するユーザデータベース等を参照することなく、メール配送の可否判断ができることから、フィルタ処理をメール配送経路上の複数のサーバで分散して実行でき、よって受信者側のメールサーバの負荷を低減できるという効果が生じる。また、送信者に近いメールサーバでフィルタ処理を行うことで、無駄なトラフィックを削減できるという効果が得られる。更に、アドレスに埋め込まれた情報により、送信者にアドレスの有効条件を伝える、受信者に有益な情報を与えるなどの機能を実現できるという効果も得られる。

【００１４】

【発明の実施の形態】

以下では、図面を参照して、本発明の実施の形態を詳細に説明する。

【００１５】

図１は、本発明による電子メールシステムの構成図である。図１において、ユーザ端末１００及び１１０は、メールを送受信する。メールサーバ１２０及び１３０は、メールを中継する。アドレス発行サーバ１４０及び１５０は、ユーザにアドレスを発行する。インターネット１６０は、メールサーバ１２０及び１３０間のメールを中継する。ディレクトリ

１７０は、アドレスの登録及び検索の機能をユーザに提供する。

【００１６】

例えば、送信者のユーザ端末１００から受信者のユーザ端末１１０へメールを配送する動作は、以下のとおりである。ユーザ端末１００で作成されたメールは送信者側のメールサーバ１２０と、インターネット１６０上のメールサーバと、受信者側のメールサーバ１３０とを経由して、受信者のユーザ端末１１０まで配送される。この経路上のメールサーバ（例えば、送信者側のメールサーバ１２０）において、メールの送信者アドレス及び受信者アドレスから、埋め込まれた制御情報及び検査情報を抽出し、この情報によってメール配送の可否判断を行い、その結果に応じてメールの配送もしくはエラー処理を行うという動作を実行する。

【００１７】

図２は、本発明によるアドレス発行サーバの機能構成図である。図２によれば、アドレス発行サーバは、入力部２００と、鍵記憶部２１０と、検査情報計算部２２０と、アドレス生成部２３０と、出力部２４０とを有する。

【００１８】

入力部２００は、ユーザの端末から、制御情報を受信する。制御情報は、フォーマット情報ｅ１、有効条件ｅ２、送信者識別子ｅ３、受信者識別子ｅ４、付加情報ｅ５のうち必要なものである。

【００１９】

・フォーマット情報ｅ１とは、以下の情報ｅ２，ｅ３，ｅ４，ｅ５，ｅ６をアドレスに埋め込む形式及びそれらの利用方法を表す情報である。

・有効条件ｅ２とは、そのアドレスが有効か否かを表す条件であり、その有効性が客観的に判断できる情報（例えば期限等）である。

・送信者識別子ｅ３とは、そのアドレスへメールを送ることができるユーザを表す情報である。

・受信者識別子ｅ４とは、そのアドレス宛てに送られたメールを受け取るユーザを表す情報である。

付加情報ｅ５とは、上記以外の目的に用いる情報である。

尚、送信者／受信者とは、それぞれメールを送信／受信するユーザの端末とする。識別子とは、ユーザを一意に識別するための情報とする。

【００２０】

鍵記憶部２１０は、鍵を記憶する。

【００２１】

検査情報計算部２２０は、制御情報ｅ１，ｅ２，ｅ３，ｅ４，ｅ５と鍵とにより、検査情報ｅ６を計算する。検査情報ｅ６は、アドレスの正当性を検査するための情報とする。アドレスの正当性とは、そのアドレスがアドレス発行サーバにより発行された正しいものであるかを表すものとする。制御情報ｅ１，ｅ２，ｅ３，ｅ４，ｅ５及び検査情報ｅ６を、「埋め込み情報」と呼ぶ。

【００２２】

アドレス生成部２３０は、埋め込み情報ｅ１，ｅ２，ｅ３，ｅ４，ｅ５，ｅ６からユーザのアドレスａｄｄｒ（ｅ１，ｅ２，ｅ３，ｅ４，ｅ５，ｅ６）を生成する。

【００２３】

出力部は、アドレス生成部２３０で生成されたアドレスをユーザの端末へ送信する。

【００２４】

アドレス発行サーバにより生成可能なアドレスを「埋め込みアドレス」と呼び、それ以外のアドレスを「通常アドレス」と呼ぶ。また、鍵記憶部２１０には、外部からアクセスできないものとする。

【００２５】

図３は、本発明によるメールサーバの機能構成図である。図３によれば、メールサーバは、埋め込み情報抽出部３００と、鍵記憶部３１０と、配送可否判断部３２０と、配送制御

部３３０とを有する。
【００２６】
埋め込み情報抽出部３００は、処理すべき受信したメールを入力し、メールで指定された送信者アドレス及び受信者アドレスから埋め込み情報を抽出し、出力する。
【００２７】
鍵記憶部３１０は、鍵を記憶する。
【００２８】
配送可否判断部３２０は、埋め込み情報と鍵とを入力し、メール配送可否判断の結果を出力する。
【００２９】
配送制御部３３０は、メールを入力し、配送可否判断部３２０からの出力に応じて、メール配送処理（正常処理）を実行するか又はエラーメールの返送等のエラー処理を実行する。
【００３０】
図３の構成に基づく本発明の電子メールシステムの動作は、以下に示されるとおりである。ユーザＡがユーザＢにメールを送る場合を例にとって、説明する。
【００３１】
送信者であるユーザＡは、ユーザ端末１００を用いてメールを送信する。送信されたメールは、メールサーバ１２０で受信される。メールサーバ１２０は、フィルタ処理を行い、配送可と判断されたメールはメールサーバ１３０へ送信する。メールサーバ１３０は、必要ならば１２０と同様の処理を行い、配送可と判断された場合は、送信者Ｂのユーザ端末１１０へメールを送信する。
【００３２】
次に、メールサーバ１２０におけるフィルタ処理を、図３を用いて説明する。
【００３３】
処理すべき受信されたメールは、埋め込み情報抽出部３００及び配送制御部３３０へ通知される。埋め込み情報抽出部３００は、メールで指定された送信者アドレス及び受信者アドレスから埋め込み情報を抽出し、配送可否判断部３２０へ通知する。配送可否判断部３２０は、埋め込み情報抽出部３００から通知された埋め込み情報と、鍵記憶部３１０から読み出した鍵とを用いて、メール配送の可否判断を行い、この結果を配送制御部３３０へ通知する。配送制御部３３０は、配送可否判断部３２０から通知された配送可否判断の結果に基づいて、これが配送可の場合にはメールを送信し（通常処理）、配送不可の場合には、エラーメールを返送するなどのエラー処理を実行する。配送制御部３３０におけるメール配送処理は、通常のメール配送エージェント（ＭＴＡ）と同様であり、この動作については既知であるので、本明細書ではその説明を省略する。尚、宛先が複数の場合には、それぞれの宛先について処理を行う。
【００３４】
アドレス発行サーバとメールサーバにおける処理の詳細を、以下の４つの実施例を用いて説明する。
【００３５】
［実施例１］
実施例１は、上述した本発明の実施の形態について、埋め込みアドレスの形式と、埋め込みアドレスの検査手順と、埋め込みアドレスの通知手順とを、具体的に定めたものとなっている。埋め込みアドレスの形式については、以下に示される通りとする。
【００３６】
図４（Ａ）は、実施例１におけるフォーマット情報ｅ１の形式である。
【００３７】
ｅ１は、８ビットの整数とし、各ビットｂ０～ｂ７（ｂ０は最下位ビット）の意味は、以下の通りとする。
・ｂ０，ｂ１，ｂ２，ｂ３，ｂ４は、それぞれｅ６，ｅ５，ｅ４，ｅ３，ｅ２の有無（０

は無し、１は有り）を表すものとする。ただし、フォーマット情報ｅ１及び受信者識別子ｅ４は必須とし、それ以外は省略可能とする。
・ｂ５，ｂ６，ｂ７は、それぞれｅ６，ｅ３，ｅ２による検査を行うか否か（０は行わない、１は行う）を表すものとする。例えば、有効条件ｅ２は有り、送信者識別子ｅ３は有り、受信者識別子ｅ４は有り、付加情報ｅ５は無し、検査情報ｅ６は有りの場合であって、かつ、ｅ２，ｅ３，ｅ６によるアドレスの検査を行う場合、
ｂ０，ｂ１，ｂ２，ｂ３，ｂ４，ｂ５，ｂ６，ｂ７
１，　０，　１，　１，　１，　１，　１，　１
となる。
・このとき、フォーマット情報ｅ１は、
$e1 = 253 = (11111101)_2 = (fd)_{16}$
となる。ここで、$(11111101)_2$は、ｅ１＝２５３の２進数表現とし、$(fd)_{16}$は、同１６進数表現とする。
・有効条件ｅ２は、アドレスの有効期限を表すものとする。年の下２桁、月、日をそれぞれ７，４，５ビットで表し、全体を１６ビットで表す。例えば、２０１０年１１月２５日に対しては、１０，１１，２５からビット列$(0001010)_2$、$(1011)_2$、$(11001)_2$を得て、
$e2 = (0001010101111001)_2 = (1579)_{16}$
を得る。
・送信者識別子ｅ３及び受信者識別子ｅ４は、３２ビットの整数とする。
・付加情報ｅ５は、このアドレスのカテゴリを表す４ビットの整数とする。アドレスのカテゴリは受信者が任意に設定し、受信メールの振り分け等に利用するものとする。
・検査情報ｅ６は、以下の式で計算される１６ビットの整数とする。
ｅ６＝ｆ２（１６，ｈ１（ｋ１，ｆ１（ｅ１，ｅ２，ｅ３，ｅ４，ｅ５））
ここで、
ｋ１は、アドレス発行サーバが記憶する鍵である。
ｆ１（ｅ１，ｅ２，ｅ３，ｅ４，ｅ５）は、５つの引数の値を１つの整数値に符号化する関数である。
ｈ１（ｋ，ｘ）は、鍵ｋ及び値ｘを引数とする一方向性ハッシュ関数である。
ｆ２（ｗ，ｘ）は、ｘの下位ｗビットを取り出す関数である。
【００３８】
図４（Ｂ）は、上記のｅ１，ｅ２，ｅ３，ｅ４，ｅ５，ｅ６を埋め込むアドレスを、ａｄｄｒ（ｅ１，ｅ２，ｅ３，ｅ４，ｅ５，ｅ６）と表した形式である。
【００３９】
埋め込みアドレスを得る手順は、まず、埋め込み情報ｅ１，ｅ２，ｅ３，ｅ４，ｅ５，ｅ６のうち必要なものを順に並べ、アドレスに使用可能な文字列に符号化を行い、区切り文字“．”をはさんで連接し、文字“＠”とドメイン名を付加するものとする。
【００４０】
尚、実施例１では文字列への符号化は、１６進数表現を用いるものとする。例えば、
・アドレスのドメイン名が“ａ．ｂ．ｃ”である。
・$e1 = (fd)_{16} = (11111101)_2$
・$e2 = (1579)_{16}$
・$e3 = (453e5f10)_{16}$
・$e4 = (9ab23815)_{16}$
・ｅ５は無し
・$e6 = (5621)_{16}$
のときの埋め込みアドレスは、
ｆｄ．１５７９．４５３ｅ５ｆ１０．９ａｂ２３８１５．５６２１
＠ａ．ｂ．ｃとなる。
【００４１】

また、
・ｅ１＝（９４）$_{16}$＝（１００１０１００）$_{2}$
・ｅ２＝（１５７９）$_{16}$
・ｅ３は無し
・ｅ４＝（９ａｂ２３８１５）$_{16}$
・ｅ５は無し
・ｅ６は無し
のときの埋め込みアドレスは、
９４．１５７９．９ａｂ２３８１５＠ａ．ｂ．ｃ
となる。

【００４２】
図５（Ａ）は、メールサーバにおける埋め込みアドレスの検査手順のフローチャートである。

【００４３】
・５００では、受信者アドレスのフォーマット情報ｅ１を読み出す。
・５０２では、ｅ１に基づき、ｅ２，ｅ３，ｅ４，ｅ５，ｅ６を抽出する。
・５０４では、等式ｂ０＝ｂ５＝１が成り立つか否かを調べて、成り立つ場合５０８，５１０，５１２を実行し、さもなければ５１４に進む。尚、ｂ０＝ｂ５＝１は、アドレスに検査情報ｅ６が埋め込まれており、かつこれを検査することを表す。
・５０８では、鍵ｋ１を読み込む。
・５１０では、ハッシュ値ｆ２（１６，ｈ１（ｋ１，ｆ１（ｅ１，ｅ２，ｅ３，ｅ４，ｅ５））））を計算し、これをｖ１とおく。
・５１２では、ｅ６＝ｖ１を調べ、成り立つ場合は５１４へ、さもなければ、５２６へそれぞれ進む。尚、アドレスがアドレス発行サーバより発行された正しいものである場合はｅ６とｖ１の下位ビットは一致する。
・５１４ではｂ４＝ｂ７＝１を調べ、成り立つ場合は５１６に、成り立たない場合は５１８にそれぞれ進む。尚、ｂ４＝ｂ７＝１は有効条件ｅ２が埋め込まれており、かつこれを検査することを表す。
・５１６では、有効条件ｅ２を調べ、満たされる場合は５１８へ、満たされない場合は５２６へそれぞれ進む。
・５１８では、ｂ３＝ｂ６＝１を調べ、成り立つ場合には５２０に、成り立たない場合は５２４にそれぞれ進む。尚、ｂ３＝ｂ６＝１はアドレスに送信者識別子ｅ３が埋め込まれており、かつこれを検査することを表す。
・５２０では、送信者の識別子の抽出を行い、結果をｖ２に代入する。（尚、５２０の手順の詳細は、図５ｂを参照して以下で説明する。）
・５２２では、ｖ２＝ｅ３を調べ、成り立つ場合には５２４へ、成り立たない場合は５２６へそれぞれ進む。尚、ｖ２＝ｅ３は、受信者が予め指定した送信者識別子ｅ３と、メール送信者のアドレスから抽出した送信者の識別子ｖ２とが、一致していることを表す。
・５２４ではメール配送処理を実行して処理を終了する。
・５２６では、エラー処理を実行して処理を終了する。

【００４４】
図５（Ｂ）は、送信者の識別子の抽出手順のフローチャートである。

【００４５】
・５２８では、送信者アドレスのフォーマット情報ｅ１を読み出す。
・５３０では、ｅ１に基づき送信者アドレスからｅ２，ｅ３，ｅ４，ｅ５，ｅ６を抽出する。ｅ１の各ビットをｂ０，ｂ１，，，ｂ７とする。
・５３２では、ｂ０＝１を調べ、満たされる場合は５３４へ、さもなくば５４０へそれぞれ進む。尚、ｂ０＝１は、アドレスに検査情報ｅ６が埋め込まれている場合を表す。
・５３４では、鍵ｋ１を読み込む。鍵ｋ１は、送信者の属するアドレス発行サーバが保持する鍵であり、５０８で得た受信者の属するアドレス発行サーバの保持する鍵ｋ１とは異

なることに注意が必要である。
・５３６では、ハッシュ値ｆ２（１６，ｈ１（ｋ１，ｆ１（ｅ１，ｅ２，ｅ３，ｅ４，ｅ５））））を計算し、これをｖ１とおく。
・５３８では、ｅ６＝ｖ１を調べ、成り立つ場合は５４０へ、さもなければ５４２へそれぞれ進む。尚、送信者のアドレスが、アドレス発行サーバより発行された正しいものである場合は、ｅ６＝ｖ１となる。
・５４０では、ｅ４を返し処理を終了する。尚、ｅ４を返すのは以下の理由による。送信者の識別子の抽出の手順で必要としているのはメールを送信したユーザの識別子である。処理を行っているメールの送信者アドレスは、この送信者が別のメールを受け取るときに用いられるアドレスであり、そのアドレスの受信者識別子ｅ４は、送信者の識別子である。よって送信者アドレスのｅ４が送信者の識別子となる。
・５４２では、エラーを返し処理を終了する。

【００４６】
次に、図１を用いて、ユーザＡのユーザ端末１００が、ユーザＢのユーザ端末１１０へメールを送信するためのアドレス通知手順を説明する。尚、ユーザＡ及びＢには、それぞれ識別子ｉｄ（Ａ）及びｉｄ（Ｂ）が予め割り振られているものとする。

【００４７】
受信者であるユーザＢは、ユーザ端末１１０からアドレス発行サーバ１５０にアクセスして、送信者を限定しないユーザＢ宛ての埋め込みアドレス
Ｌ１＝ａｄｄｒ（ｅ１，ｅ２，ｅ３，ｅ４，ｅ５，ｅ６）
を取得する。ここで、
・ｅ１＝（１０１１０１０１）$_2$
・ｅ２は有り
・ｅ３は無し
・ｅ４＝ｉｄ（Ｂ）
・ｅ５は無し
・ｅ６は有り
とする。ユーザＢは、アドレスＬ１を、ディレクトリ１７０に登録する。

【００４８】
一方、送信者であるユーザＡは、ユーザ端末１００よりディレクトリ１７０を検索し、ユーザＢのアドレスＬ１を取得する。ユーザＡの端末は、アドレスＬ１のｅ４よりユーザＢの識別子ｉｄ（Ｂ）を抽出する。ユーザＡのユーザ端末１００は、アドレス発行サーバ１４０にアクセスし、送信者をユーザＢに限定したユーザＡ宛てのアドレスＬ２＝ａｄｄｒ（ｅ１’，ｅ２’，ｅ３’，ｅ４’，ｅ５’，ｅ６’）を取得する。ここで、
・ｅ１’＝（１１１１１１０１）$_2$
・ｅ２’は有り
・ｅ３’＝ｉｄ（Ｂ）
・ｅ４’＝ｉｄ（Ａ）
・ｅ５’は無し
・ｅ６’は有り
とする。ユーザＡのユーザ端末１００は、受信者アドレスをＬ１、送信者アドレスをＬ２としたメールＭ１を、ユーザＢの端末へ送信する。

【００４９】
ユーザＢのユーザ端末１１０は、メールＭ１の送信者アドレスＬ２のｅ４’から、ユーザＡの識別子ｉｄ（Ａ）を抽出する。ユーザＢのユーザ端末１１０は、再度、アドレス発行サーバ１５０にアクセスし、送信者をユーザＡに限定したユーザＢ宛てのアドレスＬ３＝ａｄｄｒ（ｅ１”，ｅ２”，ｅ３”，ｅ４”，ｅ５”，ｅ６”）を取得する。ここで、
・ｅ１”＝（１１１１１１０１）$_2$
・ｅ２”は有り
・ｅ３”＝ｉｄ（Ａ）

・ｅ４”＝ｉｄ（Ｂ）
・ｅ５”は無し
・ｅ６”は有り
とする。ユーザＢのユーザ端末１１０は、受信者アドレスをＬ２、送信者アドレスをＬ３としたメールＭ２を、ユーザＡのユーザ端末１００へ返信する。ユーザＡのユーザ端末１００は、メールＭ２より送信者アドレスＬ３を取得し、以後のユーザＢ宛てのアドレスとして用いる。

【００５０】
以上の手順によりユーザＡ及びＢは、互いのみからメールを送受信できる一組のアドレスＬ２及びＬ３を取得できる。

【００５１】
ところで、
・Ｌ１は、誰でもユーザＢにメールを送れるアドレス
・Ｌ２は、ユーザＢのみユーザＡにメールを送信できるアドレス
・Ｌ３は、ユーザＡのみユーザＢにメールを送信できるアドレス
である。

【００５２】
尚、Ｌ１は、送信者の限定をしていない一時的なアドレスのため、期限ｅ２を短く設定する必要がある。上記の手順は、ディレクトリを仲介したアドレス通知手順の一例であり、さまざまな変形が可能である。例えば、アドレス発行サーバ１４０及び１５０にディレクトリの機能を持たせ、ディレクトリ１７０にはそれらへのリンクを格納する構成も可能である。この構成によれば、ユーザＢは、上記Ｌ１を発行せずに、ユーザＡは、直接Ｌ３を取得することができる。

【００５３】
実施例１においては、鍵付き一方向性ハッシュ関数の出力値を比較することでアドレスの正当性の検査を行っている。ハッシュ値は高速に計算できるため、アドレスの正当性の検査も高速である。尚、鍵についてはメールサーバとアドレス発行サーバとの間で同一の鍵ｋ１を事前に共有し、それぞれの記憶部内に秘密に保持されているものとする。また、鍵を知ることなく検査情報ｅ６を計算できないことから、有効なアドレスを偽造することは困難となっている。ｅ６をランダムに選んだ場合、偶然正しい検査情報に一致する確率は小さく、この確率は検査情報のビット数を増やすことで限りなく小さくできる。また、有効なアドレスに対して可能な鍵全てを適用して鍵を割り出す総当り攻撃が可能であるが、鍵の長さを十分長く取れば攻撃は実質的に無効化できる。

【００５４】
実施例１は、本発明の実施の一例であり、各埋め込み情報のビット数や埋め込み方法は任意に選択可能である。更に、通常のアドレスからのメールを受け付けるか否か、送信者アドレスの正当性を検査するか否か、などの制御を追加することも可能である。また、ハッシュ関数によるアドレス正当性検査を、公開鍵暗号に基づく署名に置き換える変形も可能である。その場合、アドレス発行サーバが保持する鍵すなわち検査情報を計算する鍵と、メールサーバが保持する鍵すなわちアドレスの正当性を検査する鍵とは、異なったものになる。尚、公開鍵暗号に基づく署名を用いた場合には、鍵管理が容易になる代わりに検証速度は低下する。

【００５５】
［実施例２］
実施例１に対して送信者認証の機能を付加した拡張について以下に説明する。

【００５６】
認証方法は、公開鍵暗号に基づく既存の方法を用いるものとする。公開鍵暗号に基づく認証方法に関しては、既知の技術であるため説明を省略する。初期設定として、送信者であるユーザＡは、公開鍵Ｋｐ（Ａ）及び秘密鍵Ｋｓ（Ａ）の組を計算し、秘密鍵Ｋｓ（Ａ）を安全な場所に記憶する。次に、ユーザＡの識別子ｉｄ（Ａ）を以下の式で計算する。

ｉｄ（Ａ）＝ｆ２（３２，ｈ２（Ｋｐ（Ａ））

【００５７】

ここで、ｈ２は、一方向性ハッシュ関数とする。ユーザＡは、メールを送信する際に、ｉｄ（Ａ）を埋め込んだユーザＡのアドレスと同時に公開鍵Ｋｐ（Ａ）を提示する。検証者（例えばメールサーバ）は、Ｋｐ（Ａ）を用いて、メール送信者が（秘密鍵Ｋｓ（Ａ）を知る）本人であることを確認できる。また、ｉｄ（Ａ）を計算した式から、Ｋｐ（Ａ）とｉｄ（Ａ）を含んだ送信者アドレスとを結びつけることができる。以上より、送信者アドレスと、送信者であるユーザＡがそのアドレスの所有者であることの根拠となるＫｓ（Ａ）とを、結びつけることができる。

【００５８】

［実施例３］

本発明の特徴である埋め込みアドレスは、通常アドレスとの共存が可能である。メールの受信者アドレスが通常アドレスの場合は、メールサーバは、従来の配送処理を行う。また、受信者アドレスが埋め込みアドレスで、送信者アドレスが通常アドレスの場合の処理を以下に示す。実施例３によれば、アドレス発行手順及びアドレス検査手順において、送信者であるユーザＡの通常アドレスａｄｄｒ－Ａから、ユーザＡの識別子ｉｄ（Ａ）を計算する部分を付加することで実現できる。ｉｄ（Ａ）は以下の式で計算する。

ｉｄ（Ａ）＝ｆ２（３２，ｈ２（ｆ３（ａｄｄｒ－Ａ））

【００５９】

ここで、ｆ３は、文字列を整数に符号化する関数とする。また、アドレス検査手順において、埋め込みアドレスか通常アドレスかの判定が必要となる。埋め込みアドレス判定は、（ａ）アドレスのドメイン名が、埋め込みアドレス用として予め登録されたものであるか、もしくは埋め込みアドレス用に予め予約されたサブドメインを含んでいる場合、かつ（ｂ）アドレスのユーザ部分（＠より左の部分）が埋め込みアドレスのフォーマットに合致している、という条件で行う。

【００６０】

［実施例４］

以下では、付加情報ｅ５を用いて、アドレスが漏洩した場合の漏洩元特定に用いる方法を一つの例として示す。ここでは、ネットワークが盗聴の恐れのない安全な通信路を用いて構成されており、よってアドレスがメール送受信者以外の第三者に盗聴されることが無いと仮定する。

【００６１】

アドレスを発行する際に、付加情報ｅ５として、アドレスを通知するユーザの識別子を入力する。この情報により、望まない送信者からのメールが届いたときに、そのメールの受信者アドレスの付加情報ｅ５を抽出することで、最初にそのアドレスを通知したユーザ（すなわちアドレスを漏洩したユーザ）を特定できる。

【００６２】

本発明の電子メールシステムは、メールに含まれる送受信者アドレスのみでメール転送の可否判断ができるという特徴により、以下のような効果を生じる。まず、従来、受信者側のメールサーバに集中していたフィルタ処理を、メール配送経路上の複数のサーバで分散して行うことで、受信者側のメールサーバの負荷を削減できるという点がある。更に、フィルタ処理を送信者に近いサーバで行うことで、無駄なトラフィックを削減できるという点がある。

【００６３】

また、不特定の受信者に向けて無差別かつ大量に送られる広告メール等によって、受信者側のメールサーバの負荷が増大するという問題が起こっている。このようなメールは、有効なメールアドレスのリストである、アドレス名簿を用いて送信されている。アドレス名簿は、可能なアドレス全てにメールを送りエラーで返送されるものを除くことで作成されるが、アドレス名簿を作るためのメールが受信者側のメールサーバの負荷になっている。また、受信者の受信拒否設定により配送されないメールも受信者側メールサーバの負荷に

なっている。

【００６４】

これらの問題に対して本発明を適用すれば、以下のような利点を生じる。

・アドレス名簿作成のためのメールは、送信者側のメールサーバでフィルタリングできるため、受信者側メールサーバの負荷が軽減できる。

・受信者の受信拒否の意図をアドレスの有効条件として設定すれば、受信拒否されるメールも同様に送信者側でフィルタリングされるため、受信者側メールサーバの負荷とはならない。

・アドレスに期限を設けることによりアドレスが失効し、時間と共にアドレス名簿が縮小していくため、アドレス名簿を維持管理するのが困難となることがある。

【００６５】

【発明の効果】

以上説明したように、本発明においては、次のような効果を奏する。

【００６６】

第１の効果は、宛先不明メールや受信者に受信を拒否されるメールについて、受信者側のメールサーバの付加を増大させることなく、効率的にフィルタ処理できることにある。その理由は、アドレスに情報を埋め込むことで、送信者側のメールサーバやメール配送経路中の複数の場所でフィルタを実装できることである。

【００６７】

第２の効果は、宛先不明メールや受信者に受信を拒否されるメールについての無駄なトラフィックを抑制できることである。その理由は、アドレスに情報を埋め込むことで、メールが最終的な受取人もしくはその直前にあるメール受信サーバまで到達する以前に、配送経路の始点に近い段階で、フィルタ処理が行えるためである。

【００６８】

第３の効果は、送信者側でアドレスが有効か否かの判断ができることにある。その理由は、予めアドレスに有効条件の情報を埋め込んであるためである。

【００６９】

第４の効果は、アドレスが漏洩した場合に、その漏洩元に関する情報が得られることである。その理由は、予めアドレスに付加情報として、アドレスを発行先を埋め込めるためである。

【００７０】

第５の効果は、メールを、予め設定したカテゴリに基づき分類できることである。その理由は、予めアドレスに付加情報として、分類情報を埋め込めるためである。

【図面の簡単な説明】

【図１】本発明による電子メールシステムの構成図である。

【図２】本発明によるアドレス発行サーバの機能構成図である。

【図３】本発明によるメールサーバの機能構成図である。

【図４】フォーマット情報ｅ１の形式（Ａ）と、埋め込みアドレスの形式（Ｂ）とを表す説明図である。

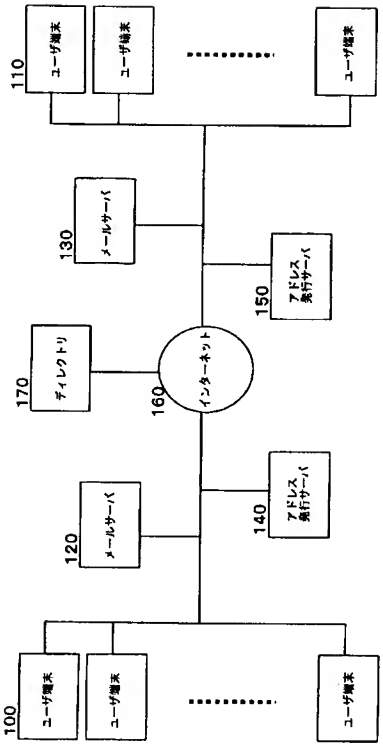
【図５】アドレス検査手順（Ａ）及びアドレス検査手順（Ｂ）のフローチャートである。

【符号の説明】

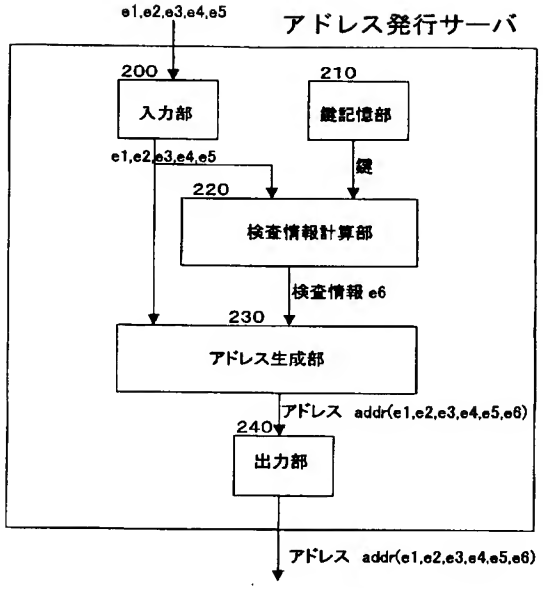
１００、１１０　ユーザ端末
１２０、１３０　メールサーバ
１４０、１５０　アドレス発行サーバ
１６０　インターネット
１７０　ディレクトリ
２００　入力部
２１０　鍵記憶部
２２０　検査情報計算部
２３０　アドレス生成部

２４０　出力部
３００　埋め込み情報抽出部
３１０　鍵記憶部
３２０　配送可否判断部
３３０　配送制御部

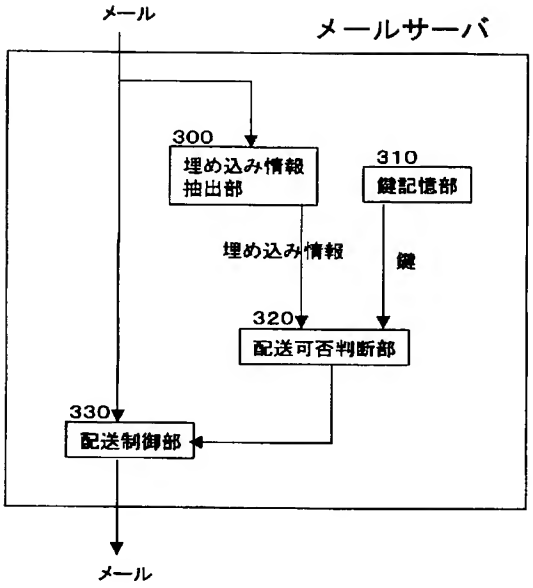
【図１】



【図２】



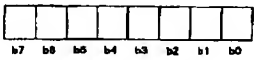
【図３】



【図４】

(A)

フォーマット情報c1の形式



b0: 検査情報(e6)の有無 (0:無し、1:有り)
b1: 付加情報(e5)の有無 (0:無し、1:有り)
b2: 受信者識別子(e4)の有無 (0:無し、1:有り)
b3: 送信者識別子(e3)の有無 (0:無し、1:有り)
b4: 有効条件(e2)の有無 (0:無し、1:有り)
b5: 検査情報(e6)による検査 (0:行わない、1:行う)
b6: 送信者識別子(e3)による検査 (0:行わない、1:行う)
b7: 有効条件(e2)による検査 (0:行わない、1:行う)

(B)

埋め込みアドレスの形式

addr(e1,e2,e3,e4,e5,e6) : [e1].[e2].[e3].[e4].[e5].[e6] @a.b.c

e1: フォーマット情報
e2: 有効条件
e3: 送信者の識別子
e4: 受信者の識別子
e5: 付加情報
e6: 検査情報 e6 = f2(16, h1(k1, f1(e1,e2,e3,e4,e5)))

(e2,e3,e5,e6)は省略可能
(e1,e4)は必須

【図５】